STUDY OF DIRECT RF INJECTION ON MICROCONTROLLER

Rashaunda Henderson and David McMasters

The University of Texas at Dallas
Dept. of Electrical Engineering
Richardson, TX 75080

6 Jun 2013

Final Report

AIR FORCE RESEARCH LABORATORY
Space Vehicles Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776

DTIC COPY
NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

Qualified requestors may obtain copies of this report from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RV-PS-TR-2013-0060 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT

//signed//   //signed//
KEITH AVERY   JAMES LYKE
Program Manager   Tech Advisor, Space Electronics Protection Branch

//signed//
CHRISTOPHER D. STOIK, Lt Col, USAF
Deputy Chief, Spacecraft Technology Division
Space Vehicles Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
06-06-2013	Final Report	20 Sept. 2011 - 20 Mar 2013

4. TITLE AND SUBTITLE
Study of Direct RF Injection on Microcontroller

5a. CONTRACT NUMBER
FA9453-11-1-0323

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62605F

6. AUTHOR(S)
Rashaunda Henderson and David McMasters

5d. PROJECT NUMBER
4867

5e. TASK NUMBER
PPM00010812

5f. WORK UNIT NUMBER
EF002775

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The University of Texas at Dallas
Dept. of Electrical Engineering
Richardson, TX 75080

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Ave. SE
Kirtland AFB, NM 87117-5776

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RVSE

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RV-PS-TR-2013-0060

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This report covers direct power injection of 8051-based microcontrollers. A test bench has been designed according to IEC 6213204 standards to test how high frequency signals impact the response of microcontroller circuits in operation.

15. SUBJECT TERMS
Microcontroller, 8051, direct power injection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	Unlimited	30	Keith Avery

19b. TELEPONE NUMBER (Include area code)

(This page intentionally left blank)

TABLE OF CONTENTS

Section	Page

LIST OF FIGURES

LIST OF TABLES

Acknowledgement

Disclaimer

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

1.0 SUMMARY

Two microcontroller circuits (Atmel LP2052 and LP216) were tested to the point of upset. Upset is defined as a reduction in voltage or shift in timing from the least significant (LSB) bit output pin (P1.0) of the microcontroller. The chip was exposed to a radio frequency (RF) signal using the direct injection method. A total of five chips were exposed to a continuous wave (CW) signal for up to 1 microsecond. At least 100 shots of pulsed power were applied to the chip from 50 to 200 MHz and each pulsed time based on a single clock cycle.

The RF signal applied to the microcontroller in pulse widths of 0.24, 0.48 or 1 microsecond. Each pulse was injected based on target locations or timing positions with respect to the microcontroller clock cycle. Because upsets are different than device failure tests, a probabilistic method was used to establish what power level affected the circuit. This information was converted to probability of effects curves and compared over frequency and the type of board that was used to test the microcontroller.

2.0 INTRODUCTION

2.1 Motivation

There is a need to develop predictive models for electronic circuits that include a mathematical relationship for RF induced effects. This information can be used to estimate how performance of devices and circuits will be altered as a function of unintentional RF power. There has been extensive research in the area of testing active circuits including chip amplifiers, complimentary metal oxide semiconductor (CMOS) inverters, and AND gates [1, 2, 3]. Recently there has been an effort to understand how electromagnetic interference (EMI) affects microcontrollers (micro-sized computers). Electric field and direct injection tests have been applied to model effects of the systems under RF power. One conclusion from the literature is that as technology scales, the bias voltage gets smaller and the susceptibility of circuits and systems increases. This work focuses on applying standard and non-standard direct injection tests to 8051-based microcontrollers.

2.2 Objectives

The project objectives involved the following:

i. Develop a direct power injection test experiment on the campus of University of Texas, Dallas (UTD).
ii. Develop the capability to perform unmonitored automated tests where large amounts of data can be gathered without human need for resetting the system or varying the inputs.

iii. Test Atmel microcontrollers that are based on the 8051 architecture (MCS-51) along with those that have advanced features including minimum power, low voltage, high speed operation and parallel processing.

iv. Test microcontrollers with RF injection on singe and multiple pins.

v. Design microcontroller programs that focus on arithmetic, logical, data transfer and branching instructions.

vi. Develop timing experiments to test how instruction type affects microcontroller susceptibility.

vii. Develop a response surface model for probability of upset due to RF power, timing, frequency, microcontroller type, test board and micro-instruction.

2.3 Organization of Report

Section 3.0 describes the experiment procedure for direct RF injection. Section 4.0 details the results of experiments with two microcontrollers tested on three boards. Section 5.0 concludes the report and Section 6.0 lists the references.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

Investigation Procedure

Two experimental procedures have been implemented and they are based on the following: 1) IEC standard [4] and 2) non-standard AFRL technique [5]. The IEC standard requires the design of a custom board and controlled impedance feed to the device under test (DUT). The Air Force Research Laboratory (AFRL) method as detailed in [5] utilizes the microcontroller development board and a custom probe to inject RF power. The test set up recommended by the International Electrotechnical Commission (IEC) is shown in Figure 1 where 50 Ω coaxial lines and a directional coupler to monitor power. The number of PCB traces is minimized to prevent stray radiation.

Figure 2 shows the block diagram used at UTD to implement the IEC set up. One additional component used is the DG535 manufactured by Stanford Research. It allows for controlled timing of the RF source and resetting the DUT as demonstrated by the AFRL experiments. This component is also useful in automating the system. Figure 3 shows the photograph of the experiment where the equipment list is detailed in Table 1.
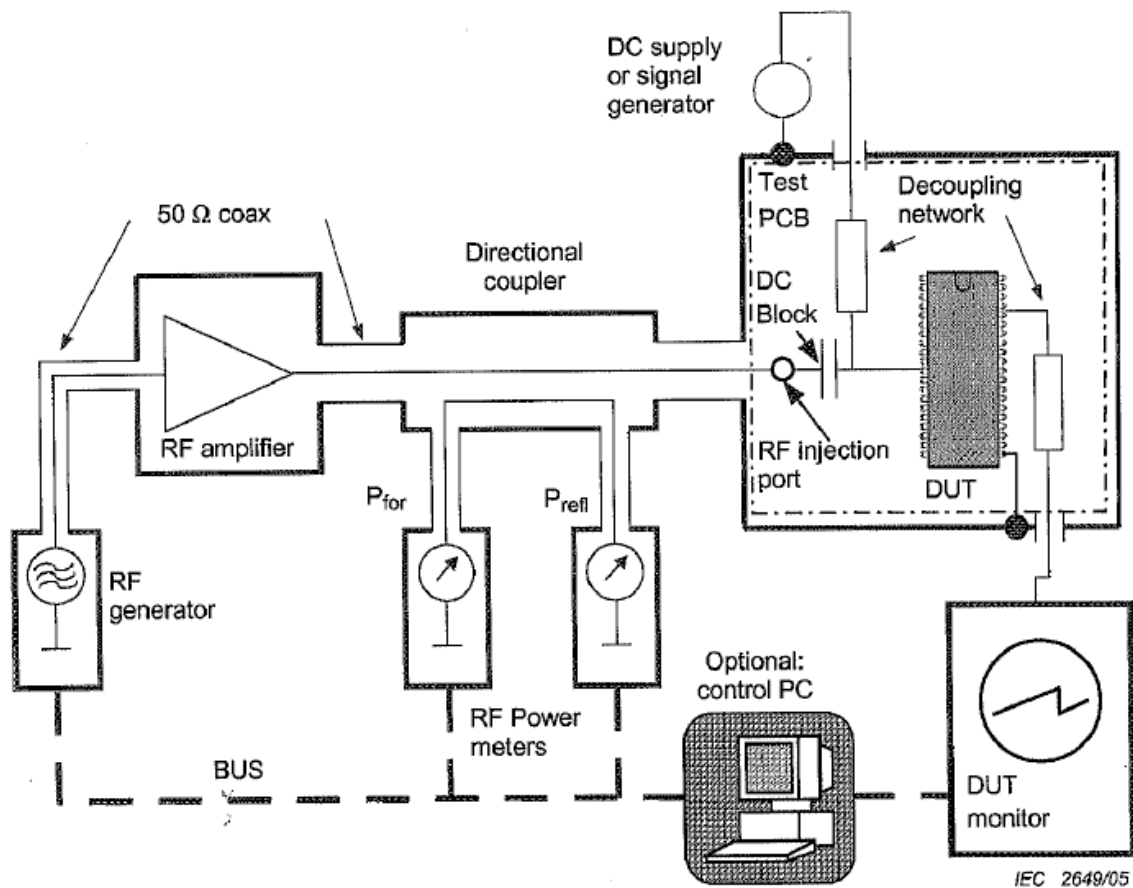
Approved for public release; distribution is unlimited.

Figure 1: Test set up recommended by IEC 62132-4.
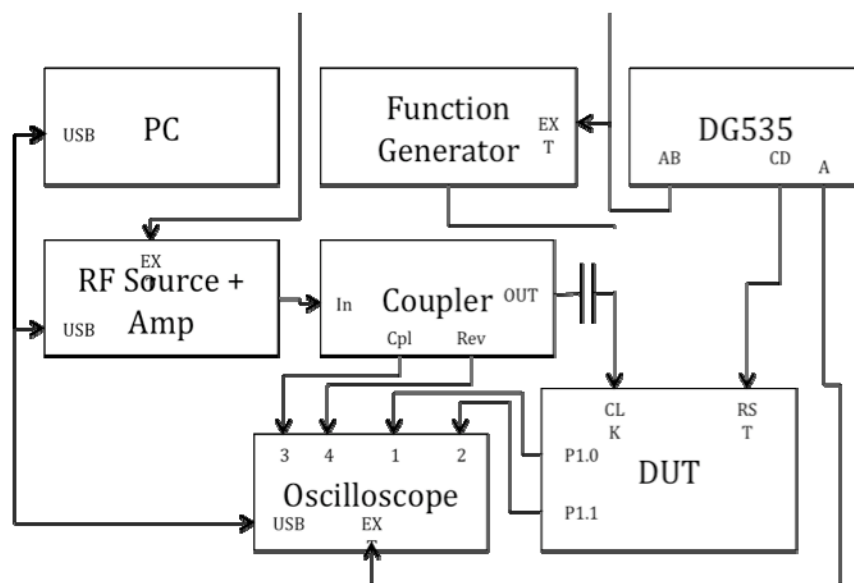
Figure 2: Block diagram for UT Dallas direct injection experiment.

Approved for public release; distribution is unlimited.

Table 1: List of equipment used in experiment at UT Dallas.

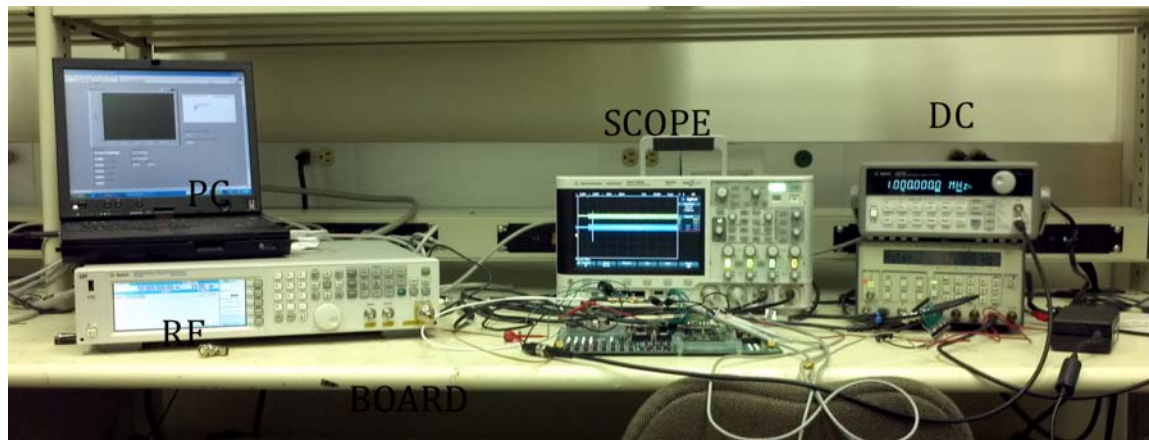| RF source	Agilent N5182A MXG
Function generator	Agilent 33120A
Oscilloscope	Agilent DSO-X 3034A 350 MHz
Directional coupler	Mini-Circuits ZFBDC20-62HP-ST
Digital delay/pulse generator	Stanford Research DG535
Software	NI Labview and AFRL ANODE
Amplifier	E&I 403LA – 3 Watts

Figure 3: Photograph of experiment.

Figure 4 shows the development board manufactured by Mikroelektronika. The Easy8051v6 development board supports 14-, 16-, 20-, 28- and 40-pin microcontrollers and has been used to program, verify and inject RF onto the microcontrollers. The extra traces to provide for board functionality can lead to excess power loss or cause unintentional RF coupling. The board has 38 light emitting diodes (LEDs) for displaying states of the pins to verify programs.

In order to inject an RF voltage to the microcontroller, a set of two dual in-line package (DIP) sockets are used as shown in Figure 5. Twenty wires are cut and soldered from the socket to another socket that will be inserted in the evaluation board. This configuration can be mounted onto the development board. Multiple pin controllers can be tested using this technique. Figure 6 shows a semi-rigid coaxial cable that connects the RF source to the custom probe. The outer conductor is stripped from the coaxial line and a ground clip (used in direct current (DC) circuits) is soldered to that stripped outer shield. A DC blocking capacitor is soldered to the RF inner conductor and is used to isolate the RF signal from the DC signal. This feed is similar to a monopole antenna that is not backed by a solid ground plane.
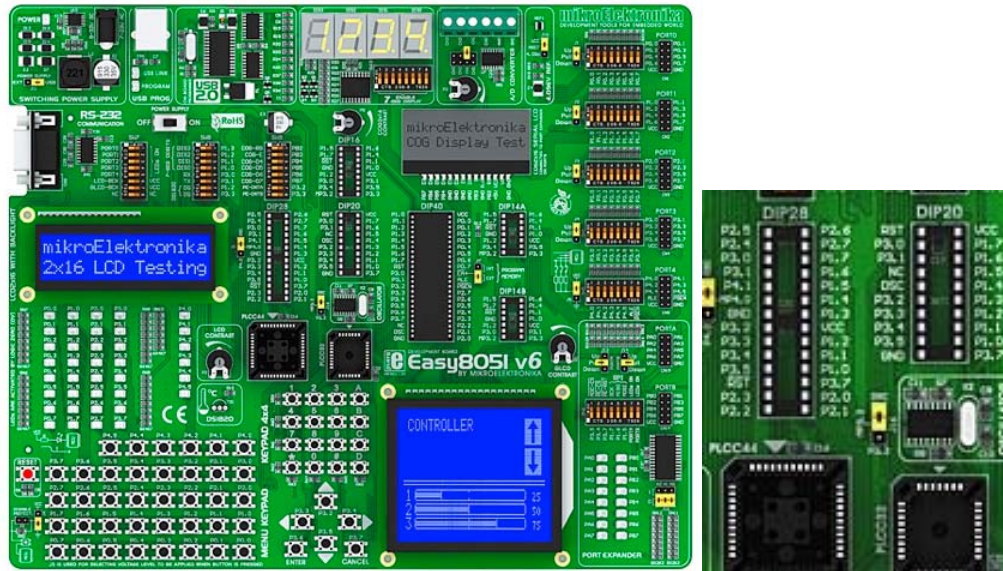
Figure 4: Easy8051 v6 development board manufactured by Mikroelektronika, close-up view of DIPs.
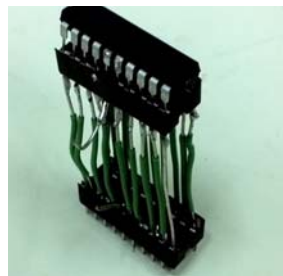
Figure 5: Two DIP sockets are used to mount the microcontroller on the development board.

Figure 6: RF probe for the development board. A semi-rigid coaxial line has ground connected to clip and DC blocking capacitor is added. The 50 ohm probe impedance is uncontrolled after the ground clip is added.

Figure 7 shows the two custom boards fabricated using FR4 substrates at UTD. The board sizes were designed to meet the IEC rule that the RF feed length to the DUT be as short as possible. The microstrip controlled impedance feed should be 1/20 of the shortest wavelength. At 200 MHz, this length is approximately 3 inches. When normalized to the permittivity of FR4 (ε_r = 4.5), that length is smaller. The smaller board was designed to meet that rule for RF injection frequencies higher than 200 MHz. The custom board can only support the microcontrollers with the same pin count, however. The silicon on insulator integrated circuit (SOIC) is soldered to the board, which makes replacing the chip difficult and requires re-soldering. Two controlled impedance feeds were designed in the board layout to inject RF on V_{cc} and the clock.

Figure 7: Two custom boards fabricated at UTD. The 50 ohm RF signal is connected to the clock signal via a SMA connector.
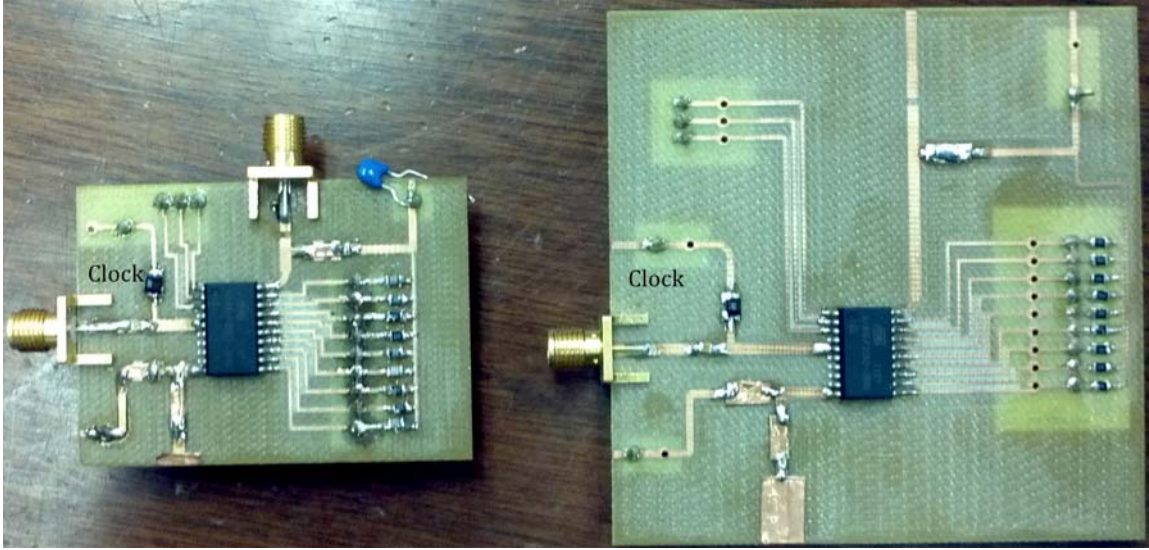
Table 2: Description and size of boards for microcontroller testing.

ID	Board	Size
1	Development board	10.5" x 8.5"
3	Custom board	3" x 3"
5	Custom board	1.7" x 2.5"

RF is physically injected onto microcontroller pins as described above. RF pulses are injected relative to the clock pulse as detailed by [5 and 6]. Seven target locations of turn on time are listed in Table 3. One complete clock cycle (TL1) is one microsecond and the shortest target location is 0.240 microseconds. Target location 1 is shown in Figure 8. Table 4 shows the frequency band, power level range and number of shots taken for each combination of the experiments. This can total up to 6000 tests, where the experiment is run automatically and all data is gathered using Labview.

Table 3: Description of target location, timing of pulse width and identification of target location.

Target Location	Pulse width (μs)	ID
Complete clock cycle	1	TL1
Logic high	0.48	TL3
1st ½ logic high	0.24	TL4
2nd ½ logic high	0.24	TL5
Logic low	0.48	TL7
1st ½ logic low	0.24	TL8
2nd ½ logic low	0.24	TL9

Approved for public release; distribution is unlimited.

Figure 8: Target location 1 that has a pulse width of 1 microsecond.

Table 4: Experiment showing frequency steps, number of shots and power level.

Board	Demo	Custom
f (MHz), in 5 MHz steps	50 - 200	
# of shots	100 - probabilistic	
Power level (dBm)	5 - 32	

Table 5: List of microcontrollers and details about packaging and programming with the development board.

Device	Pins	RAM	DIP for dev board	SOIC for custom board	Programmable
AT89LP216	16	128	Y	Y	Y
AT89LP2052	20	256	Y	Y	Y
ATtiny43U – 8 bit RISC device	20	256	N	Y	N – ultra low voltage
AT89S8253	40		Y	N	Y

Table 5 lists the microcontrollers that were considered for the RF injection experiments. We wanted to choose microcontrollers that could be programmed and tested on both the development and custom board. We narrowed down our choices to device that have been packaged as a SOIC and DIP. The two microcontrollers that achieved the requirement were the AT89LP216 and AT89LP2052.

4.0 RESULTS AND DISCUSSION

Probability of effects (P_E) curves have been generated for the AT89LP2052 and AT89LP216 microcontrollers in the SOIC package using the custom board and the DIP mounted on the Mikroelektronika board. The LP2052 is the standard microcontroller that has been tested by both UTD and AFRL, while the LP216 is a more advanced device. Initially we planned to look at a number of microcontrollers but custom board and packaged pinout limited us to the LP216. We found it difficult to locate a different microcontroller that fit the evaluation board and could follow the same SOIC pinout without having to redesign the custom board.

The RF signal is generated by a RF source and amplified using a Electronics and Innovations (E&I) amplifier that works from 150kH to 300 MHz. The RF signal was varied from 5 to 32 dBm from 50 MHz to 200 MHz. The RF continuous wave (CW) signal was set to be input during different times of the program. The least significant bit

Approved for public release; distribution is unlimited.

PIN 1.0 was connected to an Agilent oscilloscope. National Instruments Labview was used to extract the output pin data. Figure 9 shows the clock signal pin as displayed on the Agilent oscilloscope. A one microsecond RF pulse (TL1) was applied to the signal from -1 to 0 microseconds.
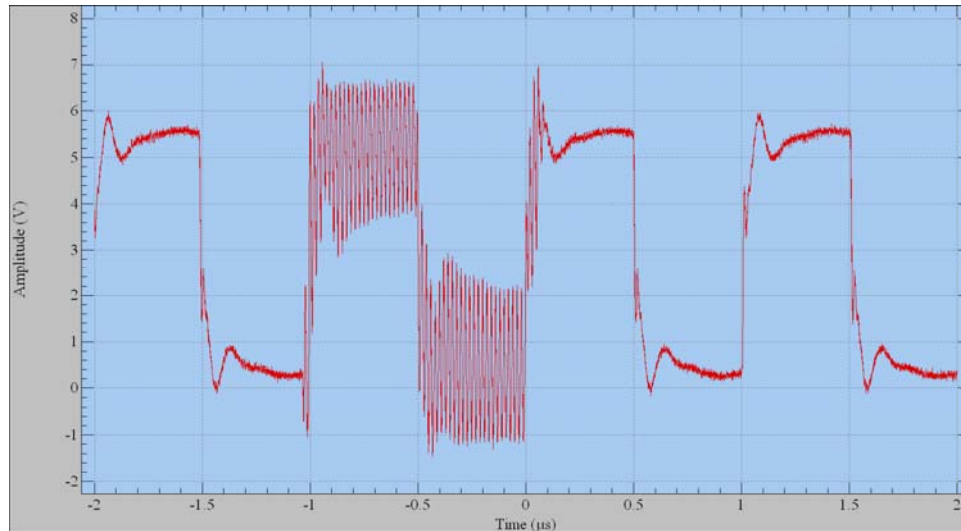

Figure 9: Block diagram of direct injection experiment with 1 microsecond RF applied to the clock signal.

The least significant bit (P1.0) is a counter. Figure 10 shows P1.0 under normal operation with a peak voltage is 5V. After RF has been applied and created an upset on the pin, the voltage has dropped down to 0.25 V as seen in Figure 11. This is described as a soft upset since P1.0 is still operating, but with a reduced voltage. By resetting the microcontroller additional tests can be conducted.
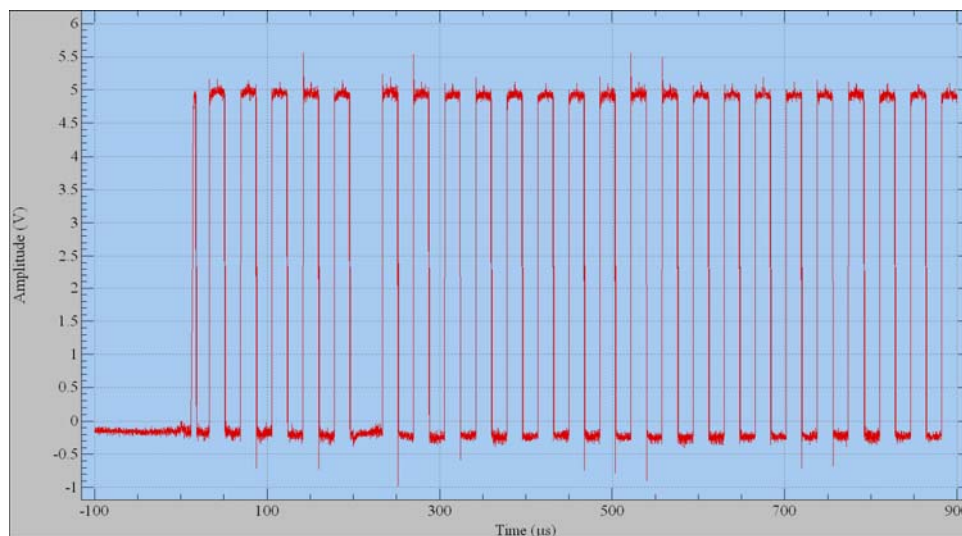

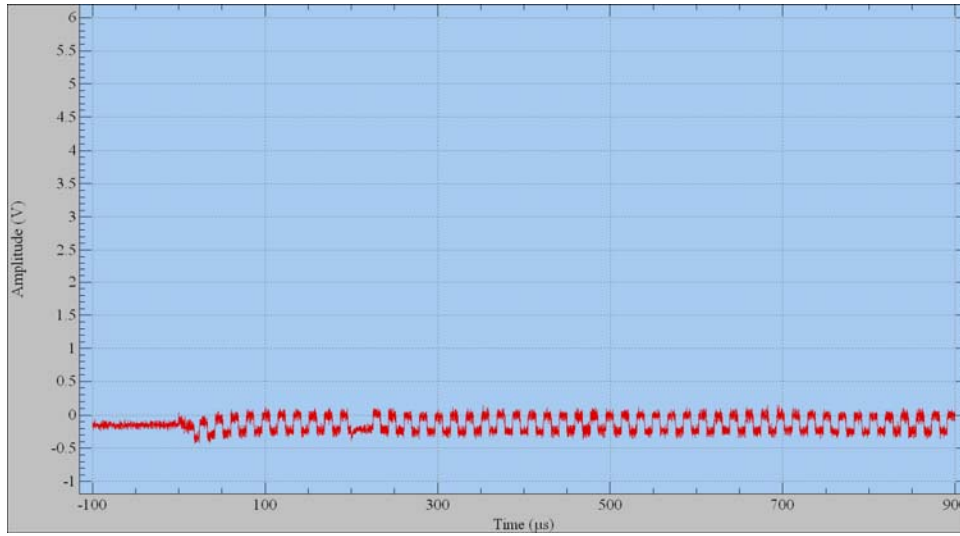**Figure 10: Least significant bit under normal operation.**

8

Figure 11: Least significant bit after RF upset.

Table 6: Extracted output using Labview.

setup	frequency	coupledvoltage	reversecoupledvoltage	Mxgpower	upset	asset
0	50	0.063	0.033	9.47	1	asset
0	50	0.066	0.033	9.926	1	asset
0	50	0.067	0.034	10.154	1	asset
0	50	0.072	0.035	10.725	1	asset
0	50	0.074	0.035	11.067	1	asset

Table 6 lists an example of the extracted results from Labview that are extracted for input in Microsoft Excel. The frequency is recorded and the voltage (coupled port and reverse coupled port) is monitored from the directional coupler. In addition the RF power in dBm from the Agilent MXG RF source is included along with recognition of an upset. If an upset occurs, a 1 is recorded. If no upset occurs a 0 is recorded.

ANODE can take the voltage and upset occurrence for the experiments and produce a probability of effects curve for the 100 shots. Figure 12 shows an example of the results obtained using ANODE [5]. The x-axis defines the peak applied RF voltage and the y-axis defines the probability of an upset between 0 and 1. A blue line on the x-axis indicates the voltage where P_E = 50%. Ninety-five percent confidence interval boundaries are included with the P_E curve.

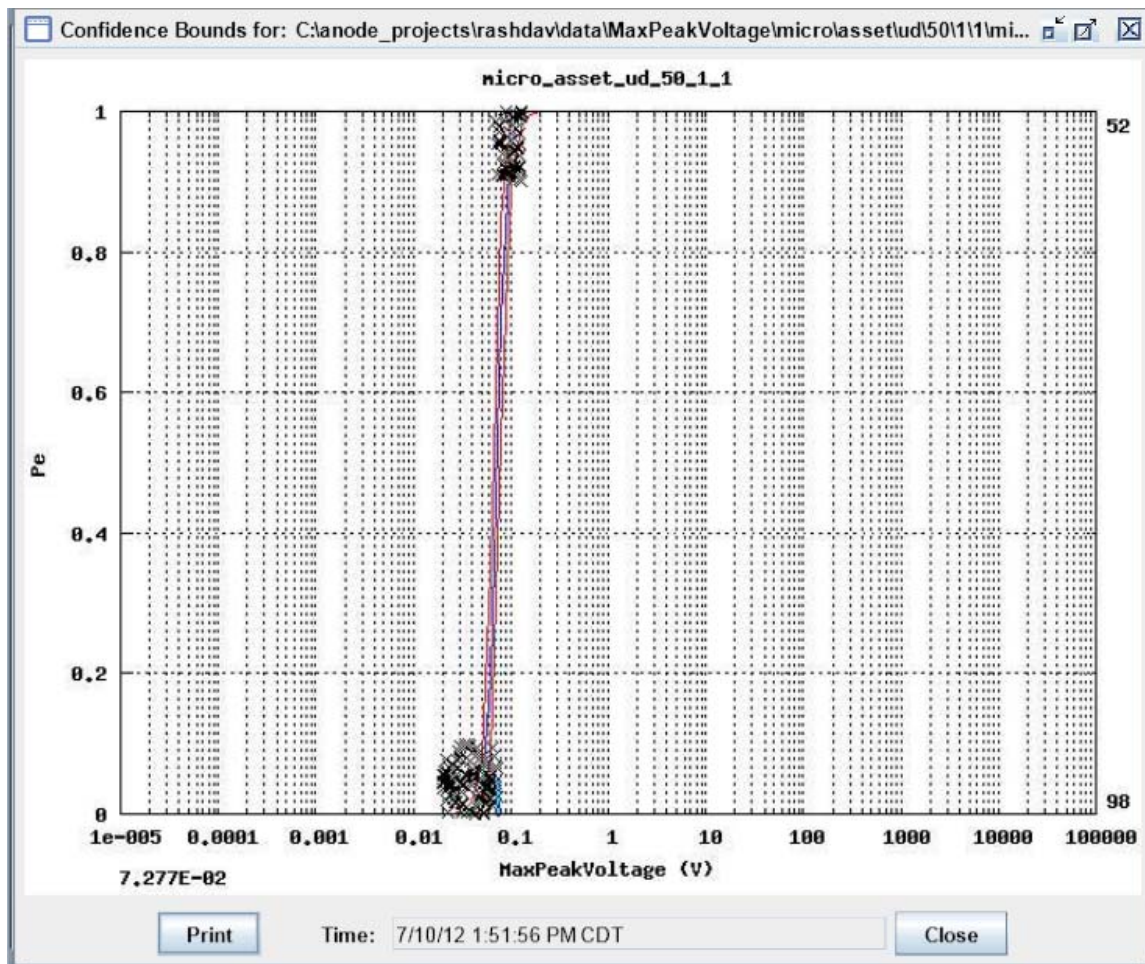Approved for public release; distribution is unlimited.

Figure 12: Example of probability of effects extracted from ANODE.

The coupler voltage listed in Figure 13 – 16 is an order of magnitude lower than the input voltage that creates an upset. Figure 13 shows the voltage at which the first upset occurred across the frequency band. The voltage at which an upset occurs for the LP2052 on the mount is shown in Figure 13. Target locations 1, 3 and 7 are at least 0.48 microseconds and the amount of voltage required to generate an upset is low and consistent across the band. As the frequency goes beyond 150 MHz, the voltage increases but there is fairly flat.

The shorter target locations (0.24 microseconds) have higher coupler voltages. TL 8 that is 1st ½ logic low required 1.5 V to create an upset at 85 MHz. At 100 MHz, TL 9 (2nd ½ logic low) requires 1 V to generate an upset as shown in Figure 14.
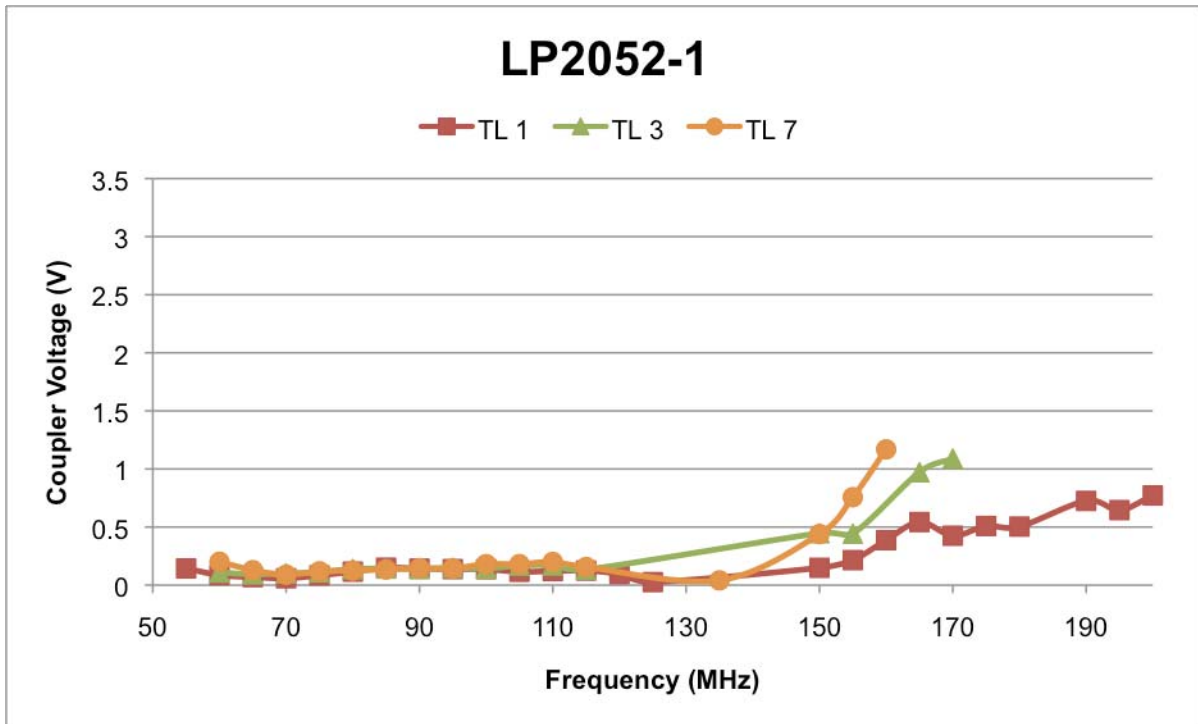
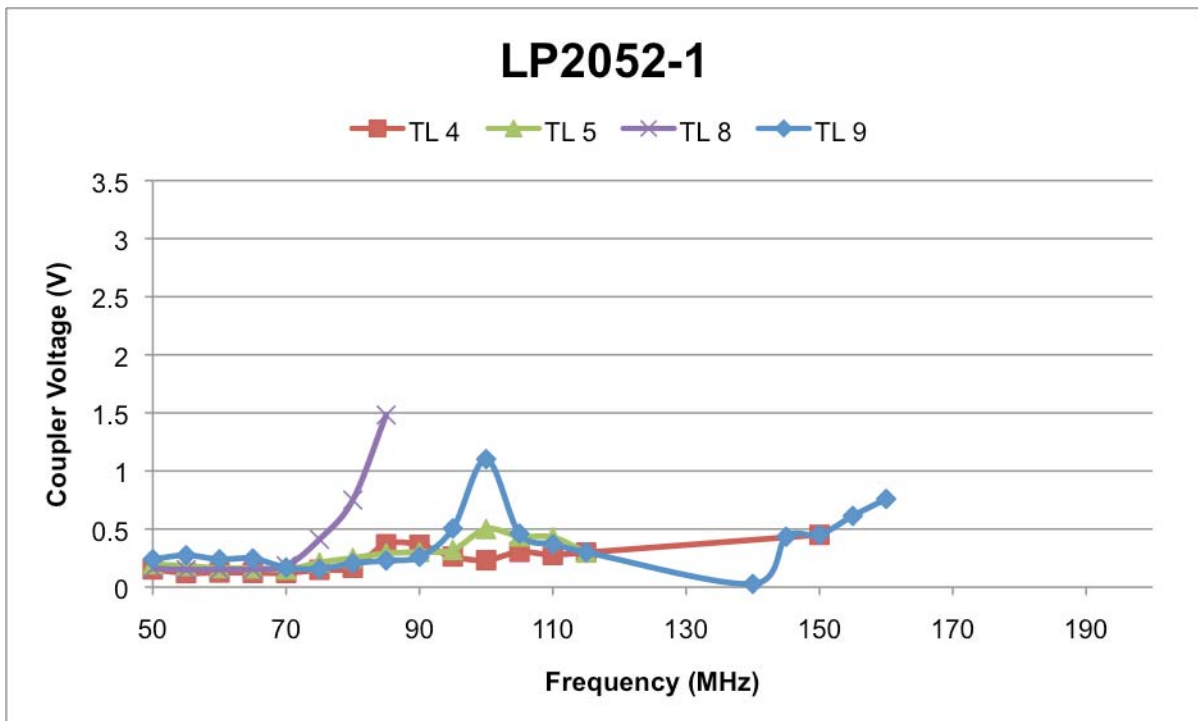**Figure 13: Coupler voltages that produce an upset for TL1, 3 and 7 on development board - 1.**

Figure 14: Coupler voltages that produce an upset for TL 4, 5, 8 and 9 on development board - 1.
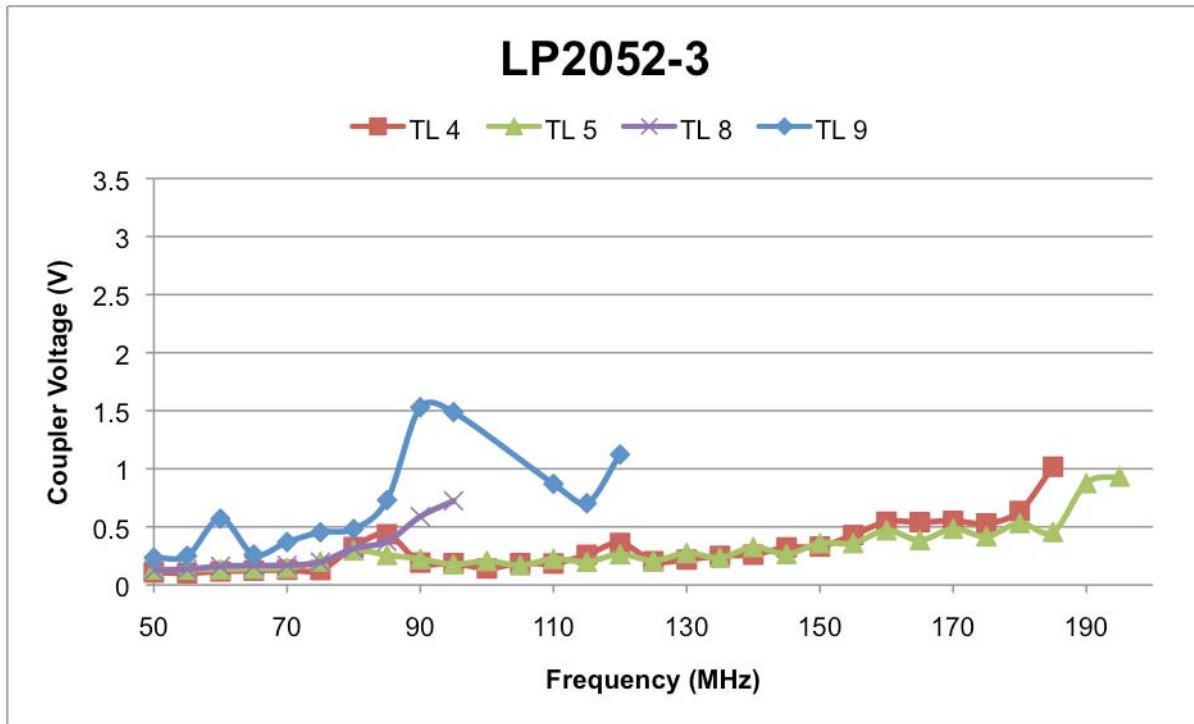
11

Figure 15: Coupler voltages that produce an upset for TL 4, 5, 8 and 9 on custom board - 3.

Figure 15 shows the coupler voltages for target locations 4, 5, 8 and 9 using custom board 3. The logic high voltages (TL 4 and TL 5) for twenty-four microseconds are flat across the band. TL 8 and TL 9 have higher voltage upsets around 90 MHz. This result is similar to what was found using the development board. Figure 16 shows that the output coupler voltage for TL 7 requires 3 V to generate an upset at 120 MHz. It is believed that there is less mismatch at the input of the custom board - 3 compared to the development board - 1 so more power can be injected into the microcontroller to test for upsets.

The LP216 microcontroller was tested and results are shown in Figure 17 and Figure 18. Two separate microcontrollers were tested during this experiment. Figure 17 shows the coupler voltage for target locations 1, 2, and 3 using the development board for microcontroller LP216. The custom board suffered from V_{dd} latch up during testing and could not be implemented in an automated format. TL 3, 4 and 5 only experienced upset from 50-55 MHz. Data for Target locations 1 and 7 have upsets up to 95 MHz. Target location 8 experiences an upset up to 80 MHz while target location 9 only has upset up to 65 MHz. The amount of voltage observed through the coupler to upset the microcontroller in target location 9 ranges from 0.5 to 1.8 V, while the voltage required for upset at target location 8 is less than 1 V.

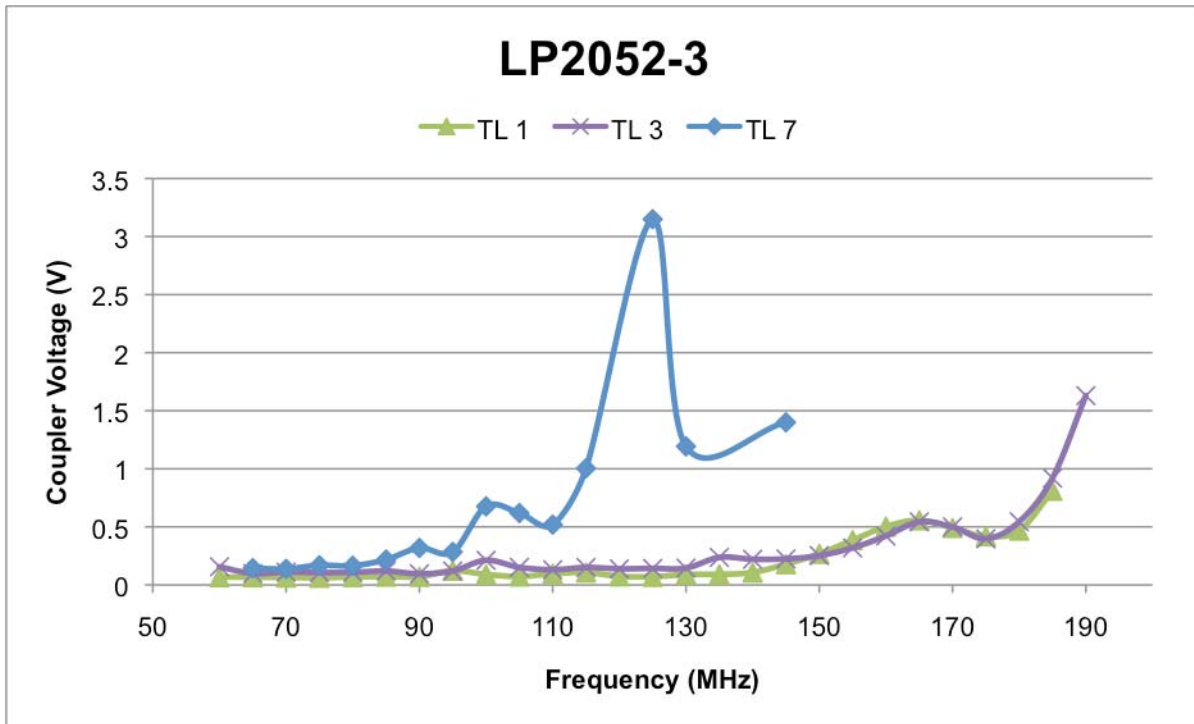Approved for public release; distribution is unlimited.

Figure 16: Coupler voltages that produce an upset for TL 1, 3 and 7 on custom board - 3.
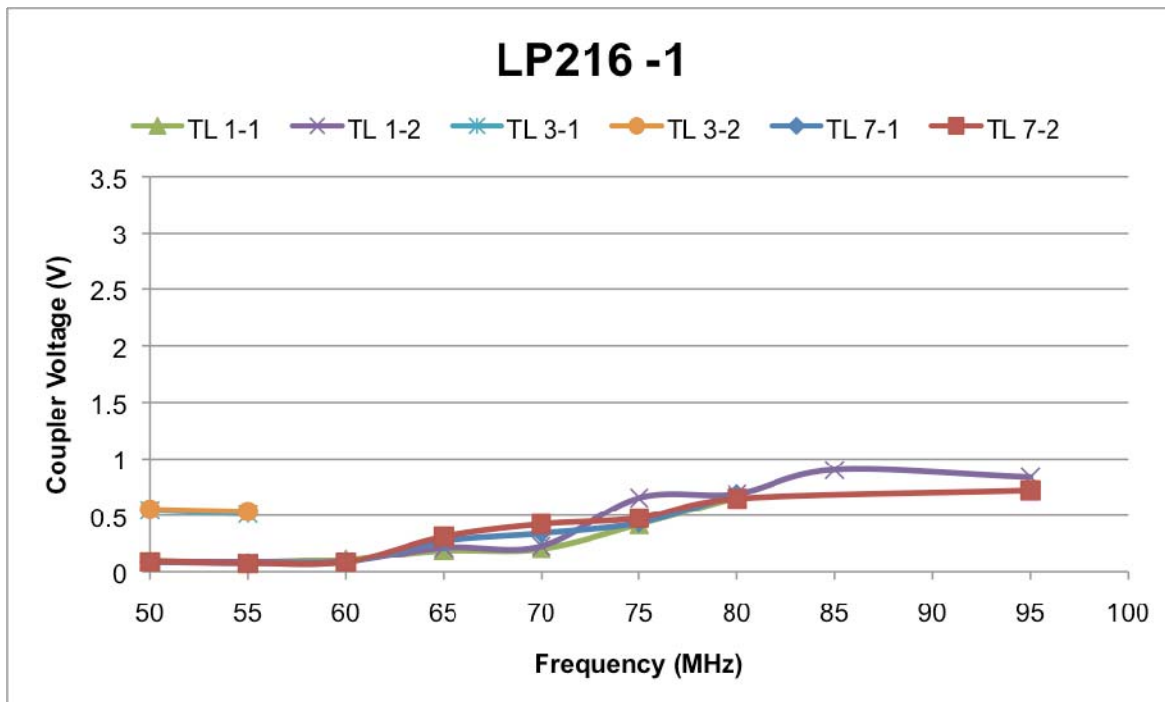

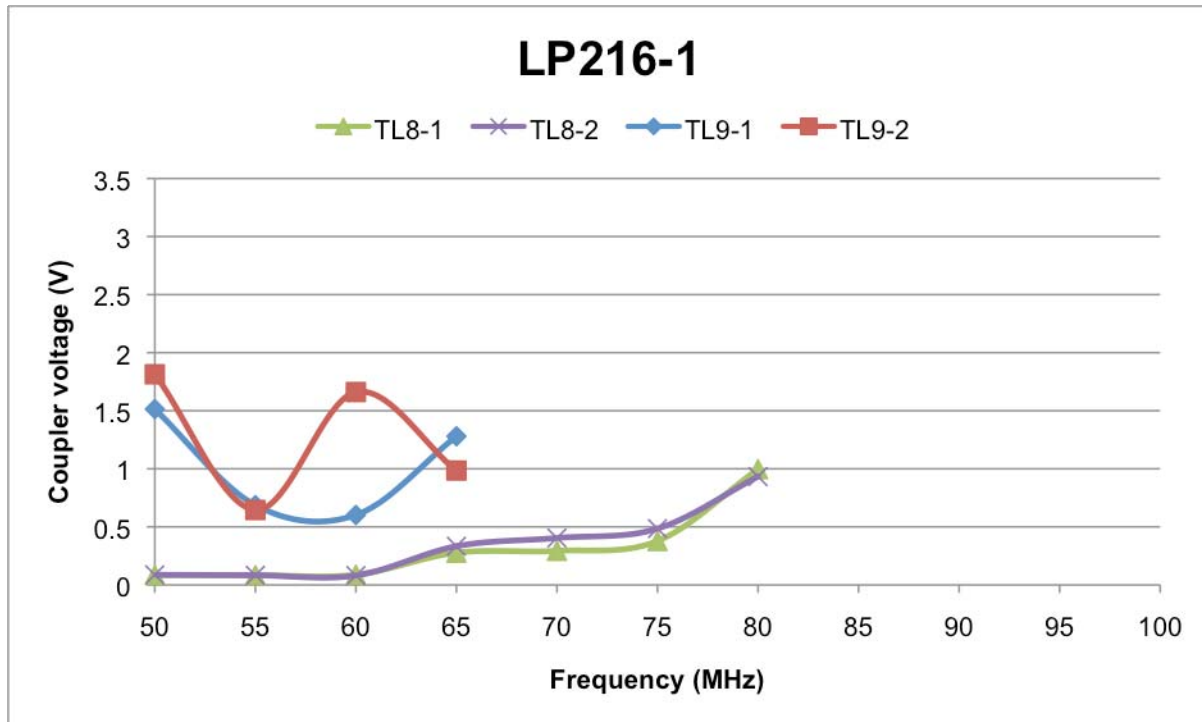**Figure 17: Coupler voltages that produce an upset for TL 1, 3, and 7 on development board. Two chips tested.**

13

LP216-1

Figure 18: Coupler voltages that produce an upset for TL 8 and 9 on development board. Two chips tested.

5.0 CONCLUSIONS

An automated direct power injection test experiment was developed on the campus of UT Dallas. This system parallels the set up available at AFRL. The system allows for direct injection testing of microcontrollers using development board packaging or using custom boards designed after IEC 62132-4 specifications. The experiments can be run unmonitored and allow for the gathering of 5-6 hours of data of approximately 5000 RF shots. Of the two Atmel microcontrollers that were tested the LP2052 circuit was found to be more susceptible for the injected power levels. The LP216 board suffered from V_{dd} latch up and required a hard reset during each upset. More time was required to fix this problem or to find another microcontroller. Advanced devices like the ATtiny microcontroller could not be tested or programmed using the custom board and were not pursued. In order to test the microcontroller with multiple input pins, a power divider would be required, which is beyond the scope of this project. RF connectors are in place to test the V_{cc} and clock signals on the custom board.

REFERENCES

[1] D. Metzger, T. Larkin, "Probability of failure estimation using binary testing," Final Report, Kaman Sciences Corporation, January 1995.

[2] H.Y.D. Yang and R. Kollman, "Analysis of high-power RF interference on digital circuits," *Electromagnetics*, Vol. 26, pp. 87-102, 2006.

[3] J. Lawrance, "Direct injection pulse experiments on 74F08 quad input AND gates," AFRL technical report, Feb. 1999.

[4] IEC, *Integrated circuits - Measurement of electromagnetic immunity 150 kHz to 1 GHz - Part 4: Direct RF power injection method*, Feb. 21, 2006.

[5] A. Taylor, *Microcontroller (8051-Core) instruction susceptibility to intentional electromagnetic interference*, Master's thesis, The University of New Mexico, Albuquerque, NM, 2011.

[6] T. Clarke, et al., "Predictive modeling of high-power electromagnetic effects on electronics," *International Conference on Electromagnetics in Advanced Applications,* ICEAA 2011, pp. 429-431.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

AFRL – Air Force Research Laboratory

CMOS – Complimentary Metal Oxide Semiconductor

CW – continuous wave

dB – decibels

dBm – decibels referenced to a milliwatt

DG 535 - Stanford DG535 pulse generator

ε_r - relative permittivity, dielectric constant

DIP – dual in-line package

DUT – device under test

EMI – electromagnetic interference

ID – identification

IEC – International Electrotechnical Commission

LSB – least significant bit

MCS-51 – Harvard architecture microcontroller (8051)

MHz – $1X10^6$ Hertz

Ohm – measure of resistance

PCB – printed circuit board

P1.0 – pin 1.0 – least significant bit

RF – radio frequency

RISC – reduced instruction set computing

SCOPE - oscilloscope

SOIC – small outline integrated circuit

TL – target location

UT Dallas or UTD – The University of Texas at Dallas

V – voltage

W – watt of power

V_{cc}, - Collector supply voltage

V_{dd} – Drain supply voltage

GLOSSARY

ANODE – Custom AFRL tool used to calculate probability of effects curves

LP216/AT89LP216 – Atmel microcontroller – 16 pin - low-power, high performance device featuring a single-cycle 8051 CPU. Can fetch a single instruction byte from memory every clock cycle.

LP2052/AT89LP2052 – Atmel microcontroller – 20 pin – low-power, high performance device featuring a single-cycle 8051 CPU. Can fetch a single instruction byte from memory every clock cycle.

DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218   1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776   2 cys

Official Record Copy
AFRL/RVSE/Keith Avery   1 cy

(This page intentionally left blank)